Process steps

Title:	ODHS|OHA 090-005-01 Information Security Incident Reporting Process
Related to:	ODHS|OHA 090-005 Information Security Incident Management Policy
Effective date:	04/05/2021

Purpose

This process outlines the steps necessary for the Oregon Department of Human Services (ODHS) and the Oregon Health Authority (OHA) to appropriately identify and report all suspected or actual security breaches, incidents, and violations, including unauthorized or impermissible uses or disclosures when required by agency, state or federal law and requirements. An information security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Applicability

This process applies to all ODHS|OHA staff including employees, volunteers, trainees, interns, as well as contractors and partners.

As keepers of the public trust, all agency employees have a responsibility to comply with state and agency policies, administrative rule, and state and federal law. The agency takes this responsibility seriously and failure to fulfill this responsibility is not treated lightly. Employees who fail to comply with state or agency policy, administrative rule, or state and federal law may face progressive discipline, up to and including dismissal from state service.

Process Steps

1. Examples of an information security incident include but are not limited to:
   a. Unauthorized or inappropriate disclosure of protected information resulting in compromise or breach.
   b. An attack that prevents or impairs the authorized use of networks, systems or applications.
   c. Inappropriate or improper usage of information technology resources that violates agency and state policy.
2. When ODHS|OHA staff suspect, or become aware of any information security incident involving unauthorized access, loss, modification, or disclosure of agency information or systems including but not limited to, personally identifiable information (PII), protected health information (PHI), federal tax information (FTI), or Criminal Justice Information Services (CJIS) information, staff shall:
   a. Immediately notify the Information Security and Privacy Office (ISPO). Notification can be done by email, phone or using the MSC 3001 form. (Refer to contact information in References)
   b. Immediately notify their manager or supervisor of the security incident.

3. Security incidents involving suspected or the actual loss of Social Security Administration (SSA)-provided information are processed according to the following steps:
   a. ISPO notifies the SSA Regional Office or the SSA Systems Security Contact as identified in the SSA Information Exchange Agreement (IEA) within one hour of notification of the suspected or actual loss of SSA-provided information.
   b. If ISPO is unable to make contact with the SSA Regional Office or the SSA Systems Security Contact within one hour, ISPO must report the security incident to the SSA's National Network Service Center (NNSC) toll free at 877-697-4889 (select "Security and PII Reporting" from the options list).
   c. ISPO provides updates as they become available to the SSA contact as appropriate.
   d. SSA makes a determination about whether the risk presented by the breach or security incident requires the notification of the individuals whose information is involved or other remediation action.
4. Security incidents involving suspected or the actual loss of Internal Revenue Service (IRS) provided FTI information are processed according to the following steps:
   a. Upon discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents, by a federal employee, a state employee, or any other person, ISPO contacts the TIFTA Field Division Office special agent-in-charge at 801-620-7734 immediately, but no later than 24 hours after identification of a possible issue involving FTI.
   b. If unable to contact the local TIGTA Field Division, ISPO contacts the Hotline Number at 800-589-3718, TIGTA Homepage: https://www.treasury.gov/tigta, Mailing Address: Treasury Inspector General for Tax Administration Ben Franklin Station P.O. Box 589 Washington, DC 20044-0589
   c. Concurrent to notifying TIGTA, the agency notifies the Office of Safeguards by email to Safeguards mailbox, safeguardreports@irs.gov.
      A. Reports are sent electronically and encrypted via IRS-approved encryption techniques. Use the term data incident report in the subject line of the email.
      B. Do not include any FTI in the data Incident report. Even if all information is not available, immediate notification is the most important factor, not the completeness of the data incident report. Additional information is provided to the Office of Safeguards as soon as it is available.
   d. To notify the Office of Safeguards, the agency documents the specifics of the incident known at that time into a data incident report, including but not limited to:
      A. Name of agency and agency point of contact for resolving data incident with contact information.
      B. Date and time the incident occurred.
      C. Date and time the incident was discovered.
      D. How the incident was discovered.
      E. Description of the incident and the data involved, including specific data elements, if known
      F. Potential number of FTI records involved; if unknown, provide a range if possible
      G. Address where the incident occurred.
      H. IT involved (e.g., laptop, server, mainframe).
   e. As part of the data incident notification, the agency confirms to the Office of Safeguards (safeguardreports@irs.gov mailbox) whether they will or may propose an adverse or

disciplinary action against staff for an unauthorized inspection or disclosure of return information in violation of agency procedures.

A. Adverse or disciplinary actions should be interpreted to include but are not limited to admonishments, written reprimands, suspensions, reduction of job responsibilities, job reassignments, reductions in pay, and terminations.

B. Adverse or disciplinary actions should also be interpreted to include alternatives that provide for any variety of both punitive and non-punitive remedial measures.

f. The agency notifies a taxpayer in writing if the agency proposes an administrative determination as to disciplinary or adverse action against an employee arising from the employee's unauthorized inspection or disclosure of the taxpayer's return or return information. The written notice includes the date of the unauthorized inspection or disclosure of return information and the rights of the taxpayer under Internal Revenue Code (IRC) §7431.

g. The agency cooperates with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident.

5. Security incidents involving the actual loss of CJIS provided information are processed according to the following steps:
   a. The Local Agency Security Officer (LASO) promptly reports the incident information to the state CJIS Information Security Officer (CJIS ISO).
   b. The LASO uses the Security Incident Response Form provided in Appendix F of the CJIS Security Policy when reporting incidents to the Oregon State Police and the Federal Bureau of Investigations (FBI) CJIS Division.
6. Security incidents involving suspected or actual loss of any other regulated data including but not limited to Protected Health Information (PHI), is reported to the ODHS|OHA Chief Information Risk Officer (CIRO) within one hour of notification.
7. In accordance with HIPAA regulations and OHA policy 100-014, when ISPO determines that a breach has occurred, and PHI may have been acquired, accessed, used, or disclosed without appropriate authorization, the responsible OHA program, in consultation with the Privacy Office:
   a. Provides written notice of the breach to the affected individual or individuals no more than 60 days after the discovery of the breach; and
   b. Provides ISPO with documentation that notice has been provided.
8. ISPO ensures identified remediation actions are performed as required by data owners, including but not limited to, SSA, IRS, and CJIS.
9. ISPO reports all information security incidents occurring within ODHS|OHA to Enterprise Information Services (EIS) Cyber Security Services (CSS), in accordance with the Statewide Information and Cyber Security Standards.

References

Statewide Information Security Plan

Center for Internet Security Top Twenty Critical Security Controls

45 CFR 160 and 164

Criminal Justice Information Systems Security Standards (CJIS)
Title 26-Internal Revenue Code § 7431
IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies
MARS-E Document Suite, Version 2.0, Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4
NIST Cybersecurity Framework
Social Security Administration Information Exchange Security Requirements and Procedures
Statewide Information and Cyber Security Standards 2019
ODHS|OHA 090-005-01 Information Security Incident Reporting Process
ODHS|OHA 090-005-02 Information Security Incident Reporting Process Map

Forms referenced
MSC 3001 DHS|OHA Privacy/Security Incident Report

Related policies
DAS 107-004-052 Information Security Policy
DAS 107-004-120 Information Security Incident Response Policy
ODHS|OHA 090-005 Information Security Incident Management
OHA 100-014 Report and Response to Privacy and Security Incidents

Contact
Information Security and Privacy Office
Security 503-945-6812
Dhsinfo.security@dhsoha.state.or.us

Process History
Version 1 (Joint DHS|OHA) 09/11/2017
Version1 DHS|OHA reviewed annually 09/12/2018
Version 1 DHS|OHA review annually 09/07/2019
Version 2 ODHS|OHA revised 04/05/2021

Keywords
Criminal Justice Information System, CJIS, corrective action, Cyber Security Services, CSS, Enterprise Information Services, EIS, Federal Bureau of Investigations, FBI, Federal Tax Information, FTI, incident, incident reporting, Internal Revenue Service, IRS, MSC 3001, Office of the Chief Information Officer, OCIO, privacy, reporting, security, Social Security Administration, SSA, system, Treasury Inspector General for Tax Administration, TIGTA
